Exhibit 121-B

Redacted Version of Document Sought to be Sealed

Interfaces One-Pager Roadmap: Platform Foundations (CA Remediation/Legacy Login Issues) 11/28/2018, 3:18 PM

Type: Document

Interfaces One-Pager Roadmap: Platform Foundations (CA Remediation/Legacy Login Issues)

- Team **mission**
  - Ensure protection of people's information by implementing a consistent, scalable, long-term approach to API development, access grants, and secure login experience across Family of Apps
- Which **audience** are you targeting?
  - Facebook product teams responsible for creating, modifying and reviewing APIs (Software Engineers, Solution Engineers, Partner Engineers, Product Managers, Technical Program Managers, Dev Ops)
  - Extended stakeholders that support the above: Data Scientists, Lawyers, Partner Managers, Product Group Leaders
- What **customer problem**(s) will the team solve? (Feel free to use the customer problem format below)
  - I am a Facebook software/solution/partner engineer who is trying to release public and private APIs to meet my customers' scenarios quickly while being compliant with platform principles and external public commitments made, but I am not familiar with them or unsure of how to objectively apply the principles, which makes me feel confused and helpless
  - I am a product group leader/lawyer who is trying to ensure we have 100% visibility into public and private APIs across all family of apps and integrations (SDK, reverse integration) for compliance with platform principles and consent decrees, but the lack of consistent, systemic, scalable process and technical enforcement program makes me feel nervous and anxious
  - I am a data scientist who is trying to answer a legal or regulatory body inquiry on people's information shared from private or public API endpoints to third-party applications over a specified timeframe under tight deadlines, but am unable to run the queries due to lack of logging, User Identifiable Information (UII) data classification of all API endpoints, and data pipeline which makes me feel helpless and frustrated
  - I am a product group leader/lawyer who is trying to ensure the Facebook platform eliminates or mitigates all legacy login behaviors that put Facebook at risk of being out of compliance with platform principles
  - I am a customer of Facebook Login using an app that uses Gigya to help manage its authentication systems. I want to feel safe using the Facebook Login product no matter if the service is provided by an aggregator/tech provider or directly by the application developer.
- **Why** is this problem important to solve? (From user, business and FB perspective)

The CA incident in March made it clear that relying on protecting people's information through contractual enforcements only is not sufficient and enforcement through internal and external gating processes and fundamental platform infrastructure changes is a must. Until the recent introductions of manual API XFN process and pause on API release, anyone in product, partner and solution engineering teams could create new APIs or modify existing ones with limited oversight. This approach has given teams the autonomy to be agile and deliver value to customers fast. At the same time, it also makes adherence to platform principles and external public commitments, compliance with legal and regulatory requirements hard to detect and enforce. There are several processes and tools in place today, viz., PDU, Privacy XFN, Risk XFN, Security Review, Capabilities Review, etc., but teams need to engage proactively, coverage is not 100%, recommendations not logged or enforced, and do not scale across Family of Apps. Further, granting access to private APIs through whitelisting is spread across multiple tools, providing no central visibility and criteria for granting access is inconsistent. Consequently, answering legal, audit and regulatory body inquiries are either cumbersome or impossible.

Examples of API related privacy issues seen this year is in Appendix below.

What does **success** look like 6 months from now, from a user perspective? 2 years from now?

6 months:

- **Create and mandate new API Program [Workstream 2] - Completed**
  - Phase 1: API XFN Launched
    - Product: new framework supports detecting >90% of new or updated APIs. Tooling to manage private access to private APIs significantly updated and launched. Tooling to manage new API XFN process launched. Key API framework risks are addressed. Restrictions on user data apply to business APIs. FB product teams building 1st party experiences should are not blocked.
    - Process: guidelines published. All new APIs go through new approval process. All new APIs built atop new framework. All teams committed to staff maintenance for new APIs. Teams needing additional features to comply must help build that feature before moving forward. Feedback loop and SEV review process follows-up on incidents to identify root causes and make tooling / product / notification decisions.
  - Phase 2: Platform Foundations
    - New framework supports detecting 100% of new or updates APIs and non-API. Ongoing improvements to API XFN, Capabilities and platform based on API XFN learnings. Ongoing detection and enforcement of API and capabilities product ownership. Full inventory of all APIs completed. Clear separation of business and consumer app separation started.

- **Cleanup all existing APIs [Workstream 3] - Completed**
  - All APIs have meaningful value to people, businesses, and FB. Low-value or high risk APIs are removed. Access revoked to features businesses aren't actively using. Significant cleanup of access to private APIs. All APIs are moved to new, centralized oversight system. [Key interim Q4'18 milestone: all APIs either deprecated or owned by a specific team committed to long-term support, including API integrity]
- **Fulfill Public Post-CA Commitments [Workstream 4] - Completed**
  - All 6 public commitments complete (see Appendix below), including review of 800K apps and turning off data access for apps people don't use.
- **Login Legacy Issues - Completed**
  - All existential questions related to consumer experiences of Facebook Login addressed.
  - All tech providers with access to app secrets beyond a threshold are identified and formal relationships established

A more detailed list of outcomes in Appendix below.

2 years:

- **API XFN Launch**
  - Product: platforms for businesses, apps / websites, 1st party, Workplace, Oculus, etc are meaningfully separated. Connections between them can only be made through deliberately approved and built conduits. 3rd party contracts are connected to the Business Graph with specific owners.
- **Platform Foundations**
  - Clear separation of new and existing Business and consumer apps enforced across platform.

- **Login Legacy Issues**
  - All tech providers migrated to Business Login flow to establish access to business permissions directly.

5. What are your **goals and metrics** that you will use as a measure of success?

Top goals with metrics for success

- % Ents with Nontrivial Privacy Policy
- UX Excellence goals and metrics? (Goal should reflect success criteria for when the customer problem is solved): **N/A**
- What were the key factors in your **decision framework**? (E.g., revenue impact, customer value, etc.)
  - Eliminate risk exposure from existing APIs and legacy login issues through audits, reaping, and deprecations
  - Eliminate risk from future API changes through temporary pause and new infra/product features and process roll-out
  - Eliminate risk from future non-API changes through new Platform foundation work
- What percentage of the portfolio is covered by the goals?
  - 50%

6. What are the **top projects, stack ranked,** that you will execute to solve this problem?

Sheet2

Area	Work Items	Team
Cleanup all existing APIs [Workstream 3]		
	Remove unused private APIs	PPI
	Challenge existence of private APIs with low-value usage	PPI
	Remove API access from partners with zero use over past 90 days	PPI
	Audit and deprecate / transfer orphaned APIs. More info Developer Platform: Public API Deprecations	PPI
	Migrate all owned APIs to new framework to API XFN Program	PPI
	Deprecate APIs based on DS analysis	PPI
	Restrict uses of first party app session in WWW context	PPI
	Deprecation of first party app sessions	PPI
Create and mandate new API Program [Workstream 2] - Phase I (Now - Feb)		
	Connect API changes to new tooling and process	PPI
	APIs for 1st and 3rd party access are cleanly separated. 1st party APIs **cannot** be made available to 3rd parties.	PPI
	All new APIs are properly categorized and documented	PPI
	Let people keep access to their accounts in apps while expiring access to user data	Identity/PPI
	Apply commitment to expire access to detailed user data to business apps	PPI
	Support for registering Apps, capabilities and business contracts on business graph	BDG
	Capabilities Tool Usability Improvements	PPI
	API XFN Tool	DevX
Create and mandate new API Program [Workstream 2] - Phase 2 (Mar-Jun)		
	Ongoing API XFN Tooling Improvements	DevX
	Evolve infra to detect non-API changes	PPI
	Run-time detection of changes to public APIs	PPI
	Ongoing detection and enforcement of product team ownership	PPI
	Complete real-time inventory of API endpoints, permissions and mapping to products	PPI
	Ongoing Logging of usage and UII data exposed	PPI
	Additional API categorization beyond UII (e.g. reverse integrations, SDKs)	PPI
	Documentation of API commandments, best practices, and examples	PPI
	Programmatic, proactive enforcement of API development best practices	PPI
	Clear Separation of Business and Consumer App Permissions	DevX/PPI/BDG /Identity
Fulfill Public Post-CA Commitments [Workstream 4]		
	Turnoff access for unused Biz Integration apps with user data permissions	Identity
	Proactive Queuing of Tier 1 and Tier 2 Apps	DevX
LogIn Legacy Issues		
Consumer Experiences	Block App Install visibility across users	PPI
	Block apps from accessing only me content (and possibly user data)	Identity/PPI

	Stop exporting privacy model to apps	PPI
	Block/reduce access to public profile after 90 day inactivity and app uninstall	Identity/PPI
	Block apps from reading canonical IDs of non-app users	Identity/PPI
Tech Providers	Enforce Business Login Flow and expire app secrets access	Identity

- What are the **key risks?**
  - Process: The two-tier process design and current TPM HC estimates might not scale to meet all Family of Apps' requirements. Current culture of 'moving fast' might be a barrier to adoption.
  - API XFN Tool: We are building on top of Launch Manager, a new unreleased tool.
  - Coverage: The path to 100% change detection and enforcement is unclear at this point. More engineering investigations of infra architecture is needed.
- What are the key **dependencies?**
  - All product teams across Family of Apps for process and tooling adoption
  - New Tier-1 and Tier-2 API XFN teams for objective criteria enforcement of API releases and granting access
  - Launch Manager team for API XFN tooling
- What **tradeoffs** did you make?
  - What fell below your cut line, and why? N/A
  - What headcount would you want? H1'19 Developer Ecosystem and Identity Projects

---

Appendix

API Issues:

Below are examples of API related issues we have seen this year:

- We don't understand our system and lack sufficient oversight over creation and access to APIs
  - FTC is frustrated FB cannot easily answer questions about which APIs share PII with 3rd parties. Answering their questions required > 1.2 person years of time including 6 weeks of manual code review and 4 weeks of analysis.
  - Partnerships granted > 100 3rd parties access to a sensitive phone number permission in 2017
- Product teams make unforced errors
  - In 2015, a Live Video engineer shared an API that exposed News Feed with 6 partners. This remains possible today. We disclosed this to Congress as an exception to Zuck's testimony when it was uncovered in Jun'18.
  - Local made a simple code change in Aug'18 to share positive engagement on posts with developers despite updates to our own data policy disallowing this type of info sharing.
- Product teams lack platform context yet optimize locally
  - Groups launched a platform at F8'18 without properly integrating into platform privacy controls resulting in a Q2 fire drill to adapt the existing experience to their product.
- The technical foundation of our APIs doesn't allow for cleanly separating our platforms
  - Q2'18: Workplace Groups were able to bypass group security for FB's consumer platform
  - Q3'18: Local changed a Page API, side-effecting Profile API against our data policy

API XFN Program Outcomes:

- API XFN is adopted by all product groups across all Family of Apps for public APIs and access grants to private API
- FB product teams building 1st party experiences are not blocked
- Every API endpoint and capability has a clear, current product owner
- Every API endpoint is classified as first-party or third-party (and extensible to additional categories), 1st party APIs **cannot** be made available to 3rd parties.
- Every APP ID is classified as first-party or third-party, block from moving from one to the other
- Every API endpoint is classified by specific UII fields and types they emit
- Every API endpoint emits *minimum* UII fields required for the scenario
- Every private API endpoint is exposed via capabilities *only* (all existing GK/Sitevars migrated to capabilities)
- Every UII type has known access requirements
- Addition of existing or new UII fields to any private or public APIs are detected, blocked and queued for XFN review
- No unforced errors due to ent layer changes bubbling up to automatic, undetected API changes
- For every app, public and private APIs and UII types it has access to can be queried without Eng and DS support
- For every business, apps they own, public and private APIs they have access to and binding contracts can be queried without Eng and DS support
- Unused capabilities and apps not using capabilities they have access to are reaped out of the system regularly
- Every capability has a clear expiry date and renewed by owner periodically
- Restrictions on user data apply to business APIs

External Public Commitments:

Sheet3

	Commitment	Status	Details
1	Review our platform	In progress	(1) Partnerships leading on historical audit (2) DevOps leading on review of ~800K remaining apps. Product spent > 2 months updating tooling and process to support Ops.
2	Inform people about apps that misused their dataTell people about data misuse	In progress	Ongoing commitment to inform people when audit finds apps misusing data. Currently includes 2 3rd party apps and View As (upcoming)
3	Turnoff access for unused apps	In progress	Revoking access in May/June led to Zuck escalations from Gaming partners. Currently carrying risk by extending access with untrusted signals. Facebook Login team spent 3 months making product changes allowing people to access their accounts in apps even when data access is expired - beta testing starts Oct'18. Major outstanding risk: 50K apps considered "business integrations" can access user profile data without being turned off.

4	Restrict Facebook Login data	In progress	Product changes complete, reviewed with Schrep in Apr'18. Developer migration period ends Jan'19.
5	Encourage people to manage apps they use	Complete	App Settings changes and CTA launched Apr'18
6	Reward people who find vulnerabilities	In progress	Program still being developed

Legacy Login Issues:

Iarc onvi Developer Platform: Risky Legacy Issues

THREAD CLASS
document

CREATED
2018-11-28T20:18:45+00:00

UPDATED
2019-06-10T16:26:49+00:00

LINK
https://fb.quip.com/vrVbAHPgSpVD

SHARED FOLDERS
H1 2019 Roadmaps

EXPANDED USERS
[redacted]

USERS
–

URLS
- https://fb.facebook.com/groups/1902146423152074/permalink/1914855108547872/
- https://fb.quip.com/pU4BAbDFni0M
- https://fb.quip.com/oHhMAiLWizhO
- https://fb.quip.com/3THRAYX7FIZY

[redacted]dited at 2018-11-28T20:18:47.907Z

- Sheet2 updated
- Sheet3 updated
- Interfaces One-Pager Roadmap: Platform Foundations (CA Remediation/Legacy Login Issues)
- Team **mission**
- Ensure protection of people's information by implementing a consistent, scalable, long-term approach to API development, access grants, and secure login experience across Family of Apps
- Which **audience** are you targeting?
- Facebook product teams responsible for creating, modifying and reviewing APIs (Software Engineers, Solution Engineers, Partner Engineers, Product Managers, Technical Program Managers, Dev Ops)
- Extended stakeholders that support the above: Data Scientists, Lawyers, Partner Managers, Product Group Leaders
- What **customer problem**(s) will the team solve? (Feel free to use the customer problem format below)
- I am a Facebook software/solution/partner engineer who is trying to release public and private APIs to meet my customers' scenarios quickly while being compliant with

platform principles and external public commitments made, but I am not familiar with them or unsure of how to objectively apply the principles, which makes me feel confused and helpless
- I am a product group leader/lawyer who is trying to ensure we have 100% visibility into public and private APIs across all family of apps and integrations (SDK, reverse integration) for compliance with platform principles and consent decrees, but the lack of consistent, systemic, scalable process and technical enforcement program makes me feel nervous and anxious
- I am a data scientist who is trying to answer a legal or regulatory body inquiry on people's information shared from private or public API endpoints to third-party applications over a specified timeframe under tight deadlines, but am unable to run the queries due to lack of logging, User Identifiable Information (UII) data classification of all API endpoints, and data pipeline which makes me feel helpless and frustrated
- I am a product group leader/lawyer who is trying to ensure the Facebook platform eliminates or mitigates all legacy login behaviors that put Facebook at risk of being out of compliance with platform principles
- I am a customer of Facebook Login using an app that uses Gigya to help manage its authentication systems. I want to feel safe using the Facebook Login product no matter if the service is provided by an aggregator/tech provider or directly by the application developer.
- **Why** is this problem important to solve? (From user, business and FB perspective)

- The CA incident in March made it clear that relying on protecting people's information through contractual enforcements only is not sufficient and enforcement through internal and external gating processes and fundamental platform infrastructure changes is a must. Until the recent introductions of manual API XFN process and pause on API release, anyone in product, partner and solution engineering teams could create new APIs or modify existing ones with limited oversight. This approach has given teams the autonomy to be agile and deliver value to customers fast. At the same time, it also makes adherence to platform principles and external public commitments, compliance with legal and regulatory requirements hard to detect and enforce. There are several processes and tools in place today, viz., PDU, Privacy XFN, Risk XFN, Security Review, Capabilities Review, etc., but teams need to engage proactively, coverage is not 100%, recommendations not logged or enforced, and do not scale across Family of Apps. Further, granting access to private APIs through whitelisting is spread across multiple tools, providing no central visibility and criteria for granting access is inconsistent. Consequently, answering legal, audit and regulatory body inquiries are either cumbersome or impossible.
- Examples of API related privacy issues seen this year is in Appendix below.

- What does **success** look like 6 months from now, from a user perspective? 2 years from now?
- **6 months:**
- **Create and mandate new API Program [Workstream 2] - Completed**
- Phase 1: API XFN Launched
- Product: new framework supports detecting >90% of new or updated APIs. Tooling to manage private access to private APIs significantly updated and launched. Tooling to manage new API XFN process launched. Key API framework risks are addressed. Restrictions on user data apply to business APIs. FB product teams building 1st party experiences should are not blocked.
- Process: guidelines published. All new APIs go through new approval process. All new APIs built atop new framework. All teams committed to staff maintenance for new APIs. Teams needing additional features to comply must help build that feature before moving forward. Feedback loop and SEV review process follows-up on incidents to identify root causes and make tooling / product / notification decisions.
- Phase 2: Platform Foundations
- New framework supports detecting 100% of new or updates APIs and non-API. Ongoing improvements to API XFN, Capabilities and platform based on API XFN learnings. Ongoing detection and enforcement of API and capabilities product ownership. Full inventory of all APIs completed. Clear separation of business and consumer app separation started.

- **Cleanup all existing APIs [Workstream 3] - Completed**
- All APIs have meaningful value to people, businesses, and FB. Low-value or high risk APIs are removed. Access revoked to features businesses aren't actively using. Significant cleanup of access to private APIs. All APIs are moved to new, centralized oversight system. [Key interim Q4'18 milestone: all APIs either deprecated or owned by a specific team committed to long-term support, including API integrity]
- **Fulfill Public Post-CA Commitments [Workstream 4] - Completed**
- All 6 public commitments complete (see Appendix below), including review of 800K apps and turning off data access for apps people don't use.
- **Login Legacy Issues - Completed**
- All existential questions related to consumer experiences of Facebook Login addressed.
- All tech providers with access to app secrets beyond a threshold are identified and formal relationships established
- A more detailed list of outcomes in Appendix below.

- **2 years:**
- **API XFN Launch**
- Product: platforms for businesses, apps / websites, 1st party, Workplace, Oculus, etc are meaningfully separated. Connections between them can only be made through deliberately approved and built conduits. 3rd party contracts are connected to the Business Graph with specific owners.
- **Platform Foundations**
- Clear separation of new and existing Business and consumer apps enforced across platform.
- **Login Legacy Issues**
- All tech providers migrated to Business Login flow to establish access to business permissions directly.

- 5. What are your **goals and metrics** that you will use as a measure of success?
- Top goals with metrics for success
- % Ents with Nontrivial Privacy Policy
- UX Excellence goals and metrics? (Goal should reflect success criteria for when the customer problem is solved): **N/A**
- What were the key factors in your **decision framework**? (E.g., revenue impact, customer value, etc.)
- Eliminate risk exposure from existing APIs and legacy login issues through audits, reaping, and deprecations
- Eliminate risk from future API changes through temporary pause and new infra/product features and process roll-out
- Eliminate risk from future non-API changes through new Platform foundation work
- What percentage of the portfolio is covered by the goals?
- 50%

- 6. What are the **top projects, stack ranked,** that you will execute to solve this problem?
- What are the **key risks?**
- Process: The two-tier process design and current TPM HC estimates might not scale to meet all Family of Apps' requirements. Current culture of 'moving fast' might be a barrier to adoption.
- API XFN Tool: We are building on top of Launch Manager, a new unreleased tool.
- Coverage: The path to 100% change detection and enforcement is unclear at this point. More engineering investigations of infra architecture is needed.
- What are the key **dependencies?**
- All product teams across Family of Apps for process and tooling adoption
- New Tier-1 and Tier-2 API XFN teams for objective criteria enforcement of API releases and granting access
- Launch Manager team for API XFN tooling
- What **tradeoffs** did you make?
- What fell below your cut line, and why? N/A
- What headcount would you want? H1'19 Developer Ecosystem and Identity Projects

- • • •
- Appendix
- **API Issues:**
- Below are examples of API related issues we have seen this year:
- We don't understand our system and lack sufficient oversight over creation and access to APIs

- FTC is frustrated FB cannot easily answer questions about which APIs share PII with 3rd parties. Answering their questions required > 1.2 person years of time including 6 weeks of manual code review and 4 weeks of analysis.
- Partnerships granted > 100 3rd parties access to a sensitive phone number permission in 2017
- Product teams make unforced errors
- In 2015, a Live Video engineer shared an API that exposed News Feed with 6 partners. This remains possible today. We disclosed this to Congress as an exception to Zuck's testimony when it was uncovered in Jun'18.
- Local made a simple code change in Aug'18 to share positive engagement on posts with developers despite updates to our own data policy disallowing this type of info sharing.
- Product teams lack platform context yet optimize locally
- Groups launched a platform at F8'18 without properly integrating into platform privacy controls resulting in a Q2 fire drill to adapt the existing experience to their product.
- The technical foundation of our APIs doesn't allow for cleanly separating our platforms
- Q2'18: Workplace Groups were able to bypass group security for FB's consumer platform
- Q3'18: Local changed a Page API, side-effecting Profile API against our data policy

- **API XFN Program Outcomes:**
- API XFN is adopted by all product groups across all Family of Apps for public APIs and access grants to private API
- FB product teams building 1st party experiences are not blocked
- Every API endpoint and capability has a clear, current product owner
- Every API endpoint is classified as first-party or third-party (and extensible to additional categories), 1st party APIs **cannot** be made available to 3rd parties.
- Every APP ID is classified as first-party or third-party, block from moving from one to the other
- Every API endpoint is classified by specific UII fields and types they emit
- Every API endpoint emits *minimum* UII fields required for the scenario
- Every private API endpoint is exposed via capabilities *only* (all existing GK/Sitevars migrated to capabilities)
- Every UII type has known access requirements
- Addition of existing or new UII fields to any private or public APIs are detected, blocked and queued for XFN review
- No unforced errors due to ent layer changes bubbling up to automatic, undetected API changes
- For every app, public and private APIs and UII types it has access to can be queried without Eng and DS support
- For every business, apps they own, public and private APIs they have access to and binding contracts can be queried without Eng and DS support
- Unused capabilities and apps not using capabilities they have access to are reaped out of the system regularly
- Every capability has a clear expiry date and renewed by owner periodically
- Restrictions on user data apply to business APIs
- **External Public Commitments:**

- **Legacy LogIn Issues:**
- [a/c priv] Developer Platform: Risky Legacy Issues